МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Директор департамента по УР
_____Ким М.Ю.
«29» _____10_____ 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ В РАДИОЭЛЕКТРОННЫХ СИСТЕМАХ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **11.05.01 Радиоэлектронные системы и комплексы**
Направленность (профиль) / специализация: **Инженерия систем связи, локации и навигации**
Форма обучения: **очная**
Факультет: **Институт радиоэлектронной техники (ИРЭТ)**
Кафедра: **институт радиоэлектронной техники (ИРЭТ)**
Курс: **5**
Семестр: **9**
Учебный план набора 2026 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	9 семестр	Всего	Единицы
Лекционные занятия	26	26	часов
Практические занятия	18	18	часов
Лабораторные занятия	16	16	часов
Самостоятельная работа	48	48	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
	3	3	з.е.

Формы промежуточной аттестации	Семестр
Зачет с оценкой	9

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ким М.Ю.
Должность: Директор департамента по УР
Дата подписания: 29.10.2025
Уникальный программный ключ:
ed789cd8-2cc6-4431-a59e-8f386b1d44fa

Томск

Согласована на портале № 84161

1. Общие положения

1.1. Цели дисциплины

1. Целью преподавания дисциплины является изучение методов защиты и основных закономерностей передачи информации в радиоэлектронный системах.

1.2. Задачи дисциплины

1. Первой задачей дисциплины является формирование у студентов компетенций, позволяющих самостоятельно проводить математический анализ физических процессов аналоговых и цифровых устройств формирования, преобразования и обработки сигналов в устройствах защиты информации радиоэлектронных систем.

2. Второй задачей дисциплины является формирование у студентов компетенций, позволяющих самостоятельно оценивать реальные и предельные возможности пропускной способности и защищенности радиоэлектронных систем.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.

Модуль дисциплин: Модуль специализации (major).

Индекс дисциплины: Б1.В.02.ДВ.01.01.11.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		
-	-	-
Профессиональные компетенции		
ПК-7. Способен решать задачи оптимизации алгоритмов обработки сигналов в радиоэлектронных системах, в том числе с применением пакетов прикладных программ	ПК-7.1. Знает методы оптимизации существующих и новых технических решений в условиях априорной неопределенности	Знает методы оптимизации существующих и новых технических решений в условиях априорной неопределенности в радиоэлектронных системах, в том числе с применением пакетов прикладных программ
	ПК-7.2. Умеет применять современный математический аппарат для решения задачи оптимизации	Умеет применять современный математический аппарат для решения задачи оптимизации в радиоэлектронных системах, в том числе с применением пакетов прикладных программ
	ПК-7.3. Владеет методами оптимизации проектируемых радиоэлектронных систем и комплексов	Владеет методами оптимизации проектируемых радиоэлектронных систем и комплексов в радиоэлектронных системах, в том числе с применением пакетов прикладных программ

4. Объем дисциплины в зачетных единицах с указанием количества академических часов,

Согласована на портале № 84161

выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		9 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	60	60
Лекционные занятия	26	26
Практические занятия	18	18
Лабораторные занятия	16	16
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	48	48
Подготовка к защите отчета по лабораторной работе	6	6
Подготовка к лабораторной работе, написание отчета	6	6
Написание отчета по лабораторной работе	6	6
Написание отчета по практическому занятию (семинару)	6	6
Подготовка к тестированию	6	6
Подготовка к зачету с оценкой	8	8
Подготовка к защите отчета по практическому занятию	5	5
Выполнение практического задания	5	5
Общая трудоемкость (в часах)	108	108
Общая трудоемкость (в з.е.)	3	3

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
9 семестр						
1 Предмет курса. Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	4	2	4	6	16	ПК-7
2 Классические шифры	2	2	-	9	13	ПК-7
3 Шифрование с секретным ключом	6	4	4	8	22	ПК-7
4 Шифрование с открытым ключом	6	2	4	8	20	ПК-7
5 Криптографические протоколы в сетях передачи данных	6	6	4	9	25	ПК-7
6 Шифрование в современных системах связи	2	2	-	8	12	ПК-7
Итого за семестр	26	18	16	48	108	
Итого	26	18	16	48	108	

5.2. Содержание разделов (тем) дисциплины

Согласована на портале № 84161

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.
Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
9 семестр			
1 Предмет курса. Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Построение систем защиты от угрозы нарушения конфиденциальности информации. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности. Построение систем защиты от угрозы нарушения целостности информации. Защита целостности программно-аппаратной среды. Построение системы защиты от угрозы доступности информации. Защита от сбоев программно-аппаратной среды. Построение системы защиты от угрозы раскрытия параметров информационной системы. Мониторинг использования систем защиты.	4	ПК-7
	Итого	4	
2 Классические шифры	Теория классических шифров. Основные характеристики открытого текста. Классификация шифров. Классификация шифров замены. Шифры перестановки. Шифры простой замены. Система шифрования Биграммный шифр Плейфейра. Шиф р Хилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистр сдвига с линейной обратной связью.	2	ПК-7
	Итого	2	

Согласована на портале № 84161

3 Шифрование с секретным ключом	Теория шифров с секретным ключом. Блочные и поточные системы шифрования. Принципы построения блочных шифров. Стандарт шифрования данных ГОСТ. Американский стандарт шифрования данных DES. Блочный криптоалгоритм стандарт AES. Методы оценки качества алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Статистический анализ гаммы шифров. Анализ результатов тестирования. Исследование производительности шифров. Поточные режимы блочных шифров. Строительные блоки по точных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обрат ной связью по переносу. Поточный шифр HC-128. Поточный шифр Rabbit. Поточный шифр Salsa20. Поточный шифр SOSEMANUK.SERPENT и его производные. Поточный шифр F-FCSR-H. Поточный шифр Grain-128. Поточный шифр MICKEY-128. Поточный шифр Trivium. Российский блочный шифр ГОСТ в поточном режиме. Блочный шифр AES в поточном	6	ПК-7
	Итого	6	
4 Шифрование с открытым ключом	Теория шифров с открытым ключом. Асимметричные криптосистемы. Предпосылки появления асимметричных криптосистем. Обобщенная схема асимметричной крипосистемы. Алгебраическая обобщенная модель шифра. Односторонние функции. Факторизация. Дискретный логарифм. Криптосистема RSA. Основные определения и теоремы. Алгоритм RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Криптосистема Эль-Гамаля. Метод экспоненциального ключевого обмена Диффи-Хеллмана. Алгоритмы практической реализации криптосистем с открытым ключом. Алгоритм Рабина-Миллера (Rabin-Miller).	6	ПК-7
	Итого	6	

Согласована на портале № 84161

5 Криптографические протоколы в сетях передачи данных	Сети шифрованной связи. Организация сетей конфиденциальной связи. Основные термины и понятия. Угрозы сетям. Протоколы распределения ключей и их характеристики. Компрометация абонентов сети; способы построения протоколов-шифрованной связи и методы их решения. Повторное использование ключей в сетях шифрованной связи. Подходы к снижению вероятности повторного использования. Современные тенденции развития средств и методов криптографической защиты информации. Программно-аппаратная реализация современных криптографических средств. Криптографические протоколы: протоколы с посредником, арбитражные протоколы и центры доверия, самодостаточный протокол, протоколы на основе симметричной и ассиметричной криптографии, хэш-функции и протоколы, протоколы смешанных криптосистем. PGP кодирование и шифрование с открытым ключом. Цифровая подпись на PGP. Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр). Электронная подпись (ЭП). Электронная цифровая подпись (ЭЦП). Безопасность сети передачи данных на транспортном уровне SSL и TLS. Безопасность сети передачи данных на сетевом уровне IPsec. IPsec является неотъемлемой частью IPv6 Интернет-протокола следующего поколения. Транспортный режим работы. Туннельный режим работы. Способы восстановления шифрованной связи после компрометации. Подходы к локализации негативных последствий компрометации. Сети связи с открытым распределением ключей. Проблемы синхронизации в сетях.	6	ПК-7
	Итого	6	
6 Шифрование в современных системах связи	Безопасность GSM сетей. Алгоритм шифрования A5/1. Безопасность сетей WIFI. Криптографическая защита беспроводных сетей стандартов LTE. Существующие методы и стандарты защиты беспроводных сетей LTE. Моделирование технологии шифрования в сетях LTE.	2	ПК-7
	Итого	2	

Согласована на портале № 84161

Итого за семестр	26	
Итого	26	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3. – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
9 семестр			
1 Предмет курса. Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Разработка архитектуры модели безопасности информационных систем и сетей	2	ПК-7
	Итого	2	
2 Классические шифры	Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. Шиф р Хилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистр сдвига с линейной обратной связью.	2	ПК-7
	Итого	2	

Согласована на портале № 84161

3 Шифрование с секретным ключом	Блочные и поточные системы шифрования. Принципы построения блочных шиф ров. Стандарт шифрования данных ГОСТ. Американский стандарт шифро вания данных DES. Блочный криптоалгоритм стандарт AES. Методы оценки качества алго ритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Анализ результатов тестирования. Исследование производительности шифров. Поточные режимы блочных шифров. Строительные блоки по точных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обрат ной связью по переносу.	4	ПК-7
	Итого	4	
4 Шифрование с открытым ключом	Алгебраическая обобщенная модель шифра. Односторонние функции. Факторизация. Дискретный логарифм. Криптосистема RSA. Основные определения и теоремы. Алгоритм RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Криптосистема Эль-Гамаля. Метод экспоненциального ключевого обмена Диффи-Хеллмана.	2	ПК-7
	Итого	2	

Согласована на портале № 84161

5 Криптографические протоколы в сетях передачи данных	PGP кодирование и шифрование с открытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. Сжатие данных. Сеть доверия. Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр). Электронная подпись (ЭП). Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP. Безопасность сети передачи данных на транспортном уровне SSL и TLS. Протокол SSL. Принцип работы SSL. Многослойная среда протокола SSL. Протокол подтверждения подключения. Протокол изменения параметров шифра. Предупредительный протокол.- Цифровые сертификаты протокола SSL. Механизмы образования ключа для текущей сессии в SSL/TLS. Предварительные объекты секретности: NULL, RSA, анонимный Диффи-Хеллман, кратковременный Диффи-Хеллман, фиксированный Диффи-Хеллман. Алгоритмы шифрования/дешифрования. Алгоритмы хэширования. Псевдослучайная функция TLS. Главный секретный код TLS. Материал для ключей TLS. Аварийный протокол в TLS. Протокол установления соединения TLS. Безопасность сети передачи данных на сетевом уровне IPsec. Архитектура средств безопасности для IP-уровня специфицирована и функционирование IPsec	6	ПК-7
	Итого	6	
6 Шифрование в современных системах связи	Безопасность GSM сетей. Алгоритм шифрования A5/1. Безопасность сетей WIFI. Криптографическая защита беспроводных сетей стандартов LTE. Существующие методы и стандарты защиты беспроводных сетей LTE. Алгоритм аутентификации и генерации ключа. Слои безопасности. Моделирование технологии шифрования в сетях LTE.	2	ПК-7
	Итого	2	
Итого за семестр		18	
Итого		18	

5.4. Лабораторные занятия

Согласована на портале № 84161

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
9 семестр			
1 Предмет курса. Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Изучение международного стандарта безопасности информационных систем ISO. Исследование системы защиты информации «Страж NT». Система защиты информации SecretNet. Система защиты информации Dallas	4	ПК-7
	Итого	4	
3 Шифрование с секретным ключом	Стандарт шифрования данных ГОСТ. Блочный криптоалгоритм стандарт AES. Методы оценки качества алгоритмов поточного шифрования. Криптоанализ шифров гаммирования. Исследование алгоритмов поточного шифрования. Поточные режимы блочных шифров. Строительные блоки поточных шифров.	4	ПК-7
	Итого	4	
4 Шифрование с открытым ключом	Алгебраическая обобщенная модель шифра. Односторонние функции. Факторизация. Дискретный логарифм. Криптосистема RSA. Основные определения и теоремы. Алгоритм RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Криптосистема Эль-Гамаля. Метод экспоненциального ключевого обмена Диффи-Хеллмана. Алгоритмы практической реализации криптосистем с открытым ключом.	4	ПК-7
	Итого	4	

Согласована на портале № 84161

5 Криптографические протоколы в сетях передачи данных	Программно-аппаратная реализация современных криптографических средств. Криптографические протоколы: протоколы с посредником, арбитражные протоколы и центры доверия, самодостаточный протокол, протоколы на основе симметричной и ассиметричной криптографии, хэш-функции и протоколы, протоколы смешанных криптосистем. PGP кодирование и шифрование с открытым ключом. Цифровая подпись на PGP. Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр). Электронная подпись (ЭП). Электронная цифровая подпись (ЭЦП). Безопасность сети передачи данных на транспортном уровне SSL и TLS. Безопасность сети передачи данных на сетевом уровне IPsec.	4	ПК-7
	Итого	4	
Итого за семестр		16	
Итого		16	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
9 семестр				

Согласована на портале № 84161

1 Предмет курса. Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Подготовка к защите отчета по лабораторной работе	1	ПК-7	Защита отчета по лабораторной работе
	Подготовка к лабораторной работе, написание отчета	1	ПК-7	Лабораторная работа
	Написание отчета по лабораторной работе	1	ПК-7	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	1	ПК-7	Отчет по практическому занятию (семинару)
	Подготовка к тестированию	1	ПК-7	Тестирование
	Подготовка к зачету с оценкой	1	ПК-7	Зачёт с оценкой
	Итого	6		
2 Классические шифры	Подготовка к защите отчета по лабораторной работе	1	ПК-7	Защита отчета по лабораторной работе
	Подготовка к защите отчета по практическому занятию	1	ПК-7	Защита отчета по практическому занятию
	Подготовка к лабораторной работе, написание отчета	1	ПК-7	Лабораторная работа
	Написание отчета по лабораторной работе	1	ПК-7	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	1	ПК-7	Отчет по практическому занятию (семинару)
	Подготовка к тестированию	1	ПК-7	Тестирование
	Выполнение практического задания	1	ПК-7	Практическое задание
	Подготовка к зачету с оценкой	2	ПК-7	Зачёт с оценкой
	Итого	9		

Согласована на портале № 84161

3 Шифрование с секретным ключом	Подготовка к защите отчета по лабораторной работе	1	ПК-7	Защита отчета по лабораторной работе
	Подготовка к защите отчета по практическому занятию	1	ПК-7	Защита отчета по практическому занятию
	Подготовка к лабораторной работе, написание отчета	1	ПК-7	Лабораторная работа
	Написание отчета по лабораторной работе	1	ПК-7	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	1	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	1	ПК-7	Практическое задание
	Подготовка к тестированию	1	ПК-7	Тестирование
	Подготовка к зачету с оценкой	1	ПК-7	Зачёт с оценкой
	Итого	8		
4 Шифрование с открытым ключом	Подготовка к защите отчета по лабораторной работе	1	ПК-7	Защита отчета по лабораторной работе
	Подготовка к защите отчета по практическому занятию	1	ПК-7	Защита отчета по практическому занятию
	Подготовка к лабораторной работе, написание отчета	1	ПК-7	Лабораторная работа
	Написание отчета по лабораторной работе	1	ПК-7	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	1	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	1	ПК-7	Практическое задание
	Подготовка к тестированию	1	ПК-7	Тестирование
	Подготовка к зачету с оценкой	1	ПК-7	Зачёт с оценкой
	Итого	8		

Согласована на портале № 84161

5 Криптографические протоколы в сетях передачи данных	Подготовка к защите отчета по лабораторной работе	1	ПК-7	Защита отчета по лабораторной работе
	Подготовка к защите отчета по практическому занятию	1	ПК-7	Защита отчета по практическому занятию
	Подготовка к лабораторной работе, написание отчета	1	ПК-7	Лабораторная работа
	Написание отчета по лабораторной работе	1	ПК-7	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	1	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	1	ПК-7	Практическое задание
	Подготовка к тестированию	1	ПК-7	Тестирование
	Подготовка к зачету с оценкой	2	ПК-7	Зачёт с оценкой
	Итого	9		
6 Шифрование в современных системах связи	Подготовка к защите отчета по лабораторной работе	1	ПК-7	Защита отчета по лабораторной работе
	Подготовка к защите отчета по практическому занятию	1	ПК-7	Защита отчета по практическому занятию
	Подготовка к лабораторной работе, написание отчета	1	ПК-7	Лабораторная работа
	Написание отчета по лабораторной работе	1	ПК-7	Отчет по лабораторной работе
	Написание отчета по практическому занятию (семинару)	1	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	1	ПК-7	Практическое задание
	Подготовка к тестированию	1	ПК-7	Тестирование
	Подготовка к зачету с оценкой	1	ПК-7	Зачёт с оценкой
	Итого	8		
Итого за семестр		48		

Согласована на портале № 84161

Итого	48	

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности				Формы контроля
	Лек. зан.	Прак. зан.	Лаб. раб.	Сам. раб.	
ПК-7	+	+	+	+	Зачёт с оценкой, Защита отчета по лабораторной работе, Защита отчета по практическому занятию, Лабораторная работа, Отчет по лабораторной работе, Отчет по практическому занятию (семинару), Практическое задание, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
9 семестр				
Зачёт с оценкой	10	10	10	30
Защита отчета по лабораторной работе	2	2	2	6
Защита отчета по практическому занятию	2	2	2	6
Лабораторная работа	2	6	6	14
Практическое задание	4	4	4	12
Тестирование	2	2	2	6
Отчет по лабораторной работе	4	4	6	14
Отчет по практическому занятию (семинару)	4	4	4	12
Итого максимум за период	30	34	36	100
Нарастающим итогом	30	64	100	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3

Согласована на портале № 84161

< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Защита информации в радиоэлектронных системах передачи информации: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 913 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/7072 .

7.2. Дополнительная литература

1. Голиков, А. М. Защита информации в радиоэлектронных системах передачи информации: Сборник компьютерных лабораторных работ / А. М. Голиков. — Томск: ТУСУР, 2018. — 224 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/8806 .
2. Голиков, А. М. Защита информации в радиоэлектронных системах передачи информации. Часть 2. Защита от утечки информации по техническим каналам: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / А. М. Голиков. — Томск: ТУСУР, 2018. — 264 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/8860.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Голиков, А. М. Кодирование и шифрование информации в радиоэлектронных системах передачи информации. Часть 2. Шифрование: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / А. М. Голиков. — Изд. перераб. и доп. — Томск: ТУСУР, 2018. — 377 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/8846 .
2. Голиков, А. М. Защита информации в цифровых системах связи. Криптографические протоколы: Учебное пособие для студентов инженерно-технических специальностей. Курс лекций, компьютерные лабораторные и практические занятия, задание на самостоятельную работу / А. М. Голиков. — Томск: ТУСУР, 2023. — 144 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/10544.
3. Организация самостоятельной работы: Учебно-методическое пособие / Д. О. Ноздреватых, Б. Ф. Ноздреватых - 2018. 23 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/7867.

7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся

Согласована на портале № 84161

из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория радиоэлектронных систем передачи информации: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ); 634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

- Компьютер (8 шт.);
- Монитор (19” SAMSUNG 1730S) (8 шт.);
- Клавиатура (8 шт.);
- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Adobe Acrobat Reader;
- Far Manager;
- Free Pascal;
- Free Pascal Lazarus (версия 1.6);
- GIMP;
- Google Chrome;
- Microsoft Windows Server 2008;
- Microsoft Windows XP;
- Mozilla Firefox;
- OpenOffice;
- Opera;
- Opera Developer;
- PTC Mathcad 13, 14;
- Scilab;

Согласована на портале № 84161

8.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория радиоэлектронных систем передачи информации: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ); 634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

- Компьютер (8 шт.);
- Монитор (19” SAMSUNG 1730S) (8 шт.);
- Клавиатура (8 шт.);
- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Adobe Acrobat Reader;
- Far Manager;
- Free Pascal;
- Free Pascal Lazarus (версия 1.6);
- GIMP;
- Google Chrome;
- Microsoft Windows Server 2008;
- Microsoft Windows XP;
- Mozilla Firefox;
- OpenOffice;
- Opera;
- Opera Developer;
- PTC Mathcad 13, 14;
- Scilab;

8.4. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 101 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 107 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 130 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.5. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания

Согласована на портале № 84161

для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Предмет курса. Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	ПК-7	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Защита отчета по лабораторной работе	Примерный перечень вопросов для защиты лабораторных работ
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 84161

2 Классические шифры	ПК-7	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Защита отчета по лабораторной работе	Примерный перечень вопросов для защиты лабораторных работ
		Защита отчета по практическому занятию	Примерный перечень вопросов для защиты практических занятий
		Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий
3 Шифрование с секретным ключом	ПК-7	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Защита отчета по лабораторной работе	Примерный перечень вопросов для защиты лабораторных работ
		Защита отчета по практическому занятию	Примерный перечень вопросов для защиты практических занятий
		Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 84161

4 Шифрование с открытым ключом	ПК-7	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Защита отчета по лабораторной работе	Примерный перечень вопросов для защиты лабораторных работ
		Защита отчета по практическому занятию	Примерный перечень вопросов для защиты практических занятий
		Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий
5 Криптографические протоколы в сетях передачи данных	ПК-7	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Защита отчета по лабораторной работе	Примерный перечень вопросов для защиты лабораторных работ
		Защита отчета по практическому занятию	Примерный перечень вопросов для защиты практических занятий
		Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 84161

6 Шифрование в современных системах связи	ПК-7	Зачёт с оценкой	Перечень вопросов для зачета с оценкой
		Защита отчета по лабораторной работе	Примерный перечень вопросов для защиты лабораторных работ
		Защита отчета по практическому занятию	Примерный перечень вопросов для защиты практических занятий
		Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Согласована на портале № 84161

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какие три основные составляющие информационной безопасности вам известны: 1) зашифрованность, целостность, доступность; 2) конфиденциальность, закрытость, доступность; 3) конфиденциальность, целостность, защищенность; 4) конфиденциальность, целостность, доступность.
2. Какие классы АС наиболее за.щищены, согласно руководящим документам Гостехкомиссии РФ: 1) 3Б и 3А; 2) 2Б и 2А; 3) 1Д, 1Г, 1В; 4) 1Б, 1А;
3. Какая модель является моделью произвольного (дискреционного) управлению доступом: 1) Модель Белла – ЛаПадула; 2) Модель Биба; 3) Хиррисона–Руззо-Ульмана; 4) Модель Кларка – Вилсона.
4. Какая модель является моделью мандатного управлению доступом: 1) Модель Белла – ЛаПадула; 2) Модель Биба; 3) Хиррисона–Руззо-Ульмана; 4) Модель Кларка – Вилсона.
5. Перечислите три основных вида угроз информационной безопасности: 1) угроза нарушения конфиденциальности, угроза нарушения целостности, угроза нарушения защищенности; 2) угроза нарушения конфиденциальности, угроза нарушения целостности, угроза нарушения доступности; 3) угроза нарушения конфиденциальности, угроза нарушения закрытости, угроза нарушения доступности; 4) угроза нарушения зашифрованности, угроза нарушения целостности, угроза нарушения доступности
6. Какая аутентификация наиболее сильная: 1) цифровая подпись; 2) пароль; 3) биометрическая; 4) уникальный предмет;
7. Какие два основных вида требований безопасности содержат «Общие критерии»: 1) требованиях безопасности, проектирование и разработка: 2) использование ресурсов, криптографическая поддержка; 3 оценка уязвимостей, оценка задания по безопасности; 4 функциональные, требования доверия;
8. Какие межсетевые экраны используют на границе локальной сети и сети Интернет: 1) коммутаторы, функционирующие на канальном уровне; 2) сетевые или пакетные фильтры; 3) шлюзы сеансового уровня (circuit-level proxy); 4) пакетные фильтры.
9. Какие методы защиты информации используются в стандарте IEEE802.11 (WiFi): 1) PAW, EWR; 2) WER, WAP; 3) PEW, APW; 4) WEP, WPA.

Согласована на портале № 84161

10. Какие виды скремблеров являются наиболее защищенными: 1) временные; 2) частотные; 3) комбинированные; 4) поточные.

9.1.2. Перечень вопросов для зачета с оценкой

1. Выделите два основных типа межсетевых экранов. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика? Является ли один из типов межсетевых экранов более безопасным, нежели другой? Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
2. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией? Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?
3. Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.
4. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность?
5. Назовите два типа биометрических систем. Назовите основные категории атак.
6. Система защиты информации. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
7. Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности информации.
8. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
9. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности? Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?
10. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификация.
11. Методологические подходы к оценке уязвимости информации. Модель защиты системы. с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости информации. Допущения в моделях оценки уязвимости информации.
12. Методы определения требований к защите информации. Факторы, обусловливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки ин- формации. Классификация требований к средствам защиты информации.
13. Требования к защите, определяемые структурой автоматизированной системы обработки данных. Требования к защите, обусловливаемые видом защищаемой информации. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.
14. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики? Почему в политику безопасности включают отказы от защиты?
15. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?
16. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз? Что такое уязвимость? Назовите четыре цели для угроз. Может ли угроза иметь более одной цели?
17. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном? Почему порядок правил в наборе правил межсетевого экрана играет важную роль?
18. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?
19. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
20. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
21. Анализ существующих методик определения требований к защите информации.
22. Факторы, влияющие на требуемый уровень защиты информации. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и

Согласована на портале № 84161

механизмы управления механизмами непосредственной защиты. Методы формирования функций защиты. События, возникающие при формировании функций защиты.

23. Если информация очень секретна, какой метод аутентификации следует использовать? Где должны храниться записи аудита в идеальном случае?
24. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией
25. Какое скремблирование реализует данный скремблер? (аналоговое или цифровое). Какой вид частотного преобразования осуществляет данный скремблер?
26. Каковы преимущества и недостатки данного вида скремблирования? Какова разборчивость выходного сигнала? Какую полосу частот занимает выходной сигнал?
27. Способы и средства защиты информации. Способы «абсолютной системы защиты». Архитектура систем защиты информации. Требования. Общеметодологических принципов архитектуры системы защиты информации.
28. На каких системах должны устанавливаться антивирусные программы? Какой длины должны быть пароли?
29. Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?
30. Согласно ГОСТ Р ИСО/МЭК 1 - какие три группы факторов необходимо учитывать при формировании требований в области информационной безопасности?
31. Какие основные информационные активы должны быть учтены и закреплены за ответственными владельцами для обеспечения информационной безопасности организации?
32. Ключевые моменты этапа анализа рисков: (перечислите)
33. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
34. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе? Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?
35. Каким набором параметров может быть идентифицирован риск. По какой формуле может быть вычислена стоимость риска?
36. Перечислите стандарте ОК 11 классов функциональных требований.
37. Как производится вычисление потенциала нападения?
38. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

9.1.3. Примерный перечень вопросов для защиты лабораторных работ

1. 1. Какова длина ключа шифра DES?
2. 2. Какова длина ключа шифра AES?
3. Отечественный стандарт блочного шифрования ГОСТ может работать в следующих режимах. Какой из них работает как синхронный поточный шифр?
4. Какая аутентификация наиболее сильная?
5. Отечественный стандарт блочного шифрования ГОСТ может работать в следующих режимах. Какой из них работает как синхронный поточный шифр?

9.1.4. Темы лабораторных работ

1. Изучение международного стандарта безопасности информационных систем ISO. Исследование системы защиты информации «Страж NT». Система защиты информации SecretNet. Система защиты информации Dallas
2. Стандарт шифрования данных ГОСТ. Блочный криптоалгоритм стандарт AES. Методы оценки качества алгоритмов поточного шифрования. Криптоанализ шифров гаммирования. Исследование алгоритмов поточного шифрования. Поточные режимы блочных шифров. Строительные блоки поточных шифров.
3. Алгебраическая обобщенная модель шифра. Односторонние функции. Факторизация. Дискретный логарифм. Криптосистема RSA. Основные определения и теоремы. Алгоритм RSA. Процедуры шифрования и расшифрования в криптосистеме RSA.

Согласована на портале № 84161

Криптосистема Эль-Гамаля. Метод экспоненциального ключевого обмена Диффи-Хеллмана. Алгоритмы практической реализации криптосистем с открытым ключом.

4. Программно-аппаратная реализация современных криптографических средств. Криптографические протоколы: протоколы с посредником, арбитражные протоколы и центры доверия, самодостаточный протокол, протоколы на основе симметричной и ассиметричной криптографии, хэш-функции и протоколы, протоколы смешанных криптосистем. PGP кодирование и шифрование с открытым ключом. Цифровая подпись на PGP. Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр). Электронная подпись (ЭП). Электронная цифровая подпись (ЭЦП). Безопасность сети передачи данных на транспортном уровне SSL и TLS. Безопасность сети передачи данных на сетевом уровне IPsec.

9.1.5. Темы практических занятий

1. Разработка архитектуры модели безопасности информационных систем и сетей
2. Система Цезаря с ключевым словом. Биграммный шифр Плейфейра. Шиф р Хилла. Шифры сложной замены. Шифр "двойной квадрат" Уитстона. Одноразовая система шифрования. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей чисел. Линейный конгруэнтный генератор. Регистр сдвига с линейной обратной связью.
3. Блочные и поточные системы шифрования. Принципы построения блочных шиф ров. Стандарт шифрования данных ГОСТ. Американский стандарт шифро вания данных DES. Блочный криптоалгоритм стандарт AES. Методы оценки качества алго ритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Набор статистических тестов НИСТ. Исследование алгоритмов поточного шифрования. Криптоанализ шифров. Статистический анализ гаммы шифров. Анализ результатов тестирования. Исследование производительности шифров. Поточные режимы блочных шифров. Строительные блоки по точных шифров. Регистры сдвига с обратной связью. Регистры сдвига с линейной обратной связью. Регистры сдвига с обрат ной связью по переносу.
4. Алгебраическая обобщенная модель шифра. Односторонние функции. Факторизация. Дискретный логарифм. Криптосистема RSA. Основные определения и теоремы. Алгоритм RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Криптосистема Эль-Гамаля. Метод экспоненциального ключевого обмена Диффи-Хеллмана.
5. PGP кодирование и шифрование с открытым ключом. Общие сведения. Совместимость. Защищённость. Механизм работы PGP. Ключи PGP. Цифровая подпись на PGP. Сжатие данных. Сеть доверия. Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр). Электронная подпись (ЭП). Электронная цифровая подпись (ЭЦП). Аннулирования открытого ключа PGP. Безопасность сети передачи данных на транспортном уровне SSL и TLS. Протокол SSL. Принцип работы SSL. Многослойная среда протокола SSL. Протокол подтверждения подключения. Протокол изменения параметров шифра. Предупредительный протокол.- Цифровые сертификаты протокола SSL. Механизмы образования ключа для текущей сессии в SSL/TLS. Предварительные объекты секретности: NULL, RSA, анонимный Диффи-Хеллман, кратковременный Диффи-Хеллман, фиксированный Диффи-Хеллман. Алгоритмы шифрования/дешифрования. Алгоритмы хэширования. Псевдослучайная функция TLS. Главный секретный код TLS. Материал для ключей TLS. Аварийный протокол в TLS. Протокол установления соединения TLS. Безопасность сети передачи данных на сетевом уровне IPsec. Архитектура средств безопасности для IP-уровня специфицирована и функционирование IPsec
6. Безопасность GSM сетей. Алгоритм шифрования A5/1. Безопасность сетей WIFI. Криптографическая защита беспроводных сетей стандартов LTE. Существующие методы и стандарты защиты беспроводных сетей LTE. Алгоритм аутентификации и генерации ключа. Слои безопасности. Моделирование технологии шифрования в сетях LTE.

9.1.6. Примерный перечень вопросов для защиты практических занятий

1. Отечественный стандарт блочного шифрования ГОСТ может работать в следующих

Согласована на портале № 84161

режимах. Какой из них работает как синхронный поточный шифр?
2. Какие виды скремблеров являются наиболее защищенными?
3. Какая аутентификация наиболее сильная?
4. Какие методы защиты информации используются в стандарте IEEE802.11 WiFi?
5. Какие межсетевые экраны используют на границе локальной сети и сети Интернет?

9.1.7. Темы практических заданий

1. Стандарты информационной безопасности и критерии оценки безопасности систем и сетей передачи информации
2. Разработка архитектуры модели безопасности информационных систем и сетей
3. Разработка практических рекомендаций по обеспечению безопасности информационных систем
4. Законодательство в области информационной безопасности
5. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.4.

Таблица 9.4 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения

Согласована на портале № 84161

С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки

9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;
– в печатной форме с увеличенным шрифтом;
– в форме электронного документа;
– методом чтения ассистентом задания вслух;
– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 84161

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры РТС
протокол № 2 от « 9 » 10 2025 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. ИРЭТ	А.М. Заболоцкий	Согласовано, 47c2d4ff-8c0e-484c-b856-20e4ba4f0e52
Заведующий обеспечивающей каф. РТС	А.С. Аникин	Согласовано, 90a9b589-4503-47e5-999f-a5e10963c1fa
Начальник учебного управления	Г.А. Цой	Согласовано, 8a5745e4-63a0-4946-bbb0-ce4977ac113e

ЭКСПЕРТЫ:

Заведующий кафедрой, каф. СВЧиКР	А.М. Заболоцкий	Согласовано, 47c2d4ff-8c0e-484c-b856-20e4ba4f0e52
Доцент, каф. РТС	А.С. Аникин	Согласовано, 90a9b589-4503-47e5-999f-a5e10963c1fa

РАЗРАБОТАНО:

Доцент, каф. РТС	А.М. Голиков	Разработано, d76b3893-b3a9-44a5-84f8-e53e691ec9d0

Согласована на портале № 84161